ECONOMY AND FINANCE • VOL. 12. ISS. 3 • SEPT 2025 • DOI: 10.33908/EF.2025.3.4

THE TAXONOMY OF FINANCIAL CYBERCRIME

Milán Kiss – Levente Kovács[1]

ABSTRACT

One of the key elements for an effective defence against cyber-attacks is a structured classification system that helps not only legislators, regulators and financial institutions, but also customers to identify and manage threats, and can support the training of students getting familiar with the financial sector. The study undertakes a systematic approach to abuses committed in cyberspace affecting the financial sector, with particular attention to the possibilities of categorising such abuses and to defence mechanisms. In parallel with the development of the digital financial ecosystem, the number and complexity of cyber threats are also increasing dynamically. The study classifies cybercrimes according to various criteria, such as the method of attack (e.g. malicious code, phishing, exploitation of vulnerabilities), the attacker's profile (e.g. APT, organised crime, hacktivists), the type of target (e.g. natural persons, companies, critical infrastructure), the nature of the defence phase (preventive, detective, corrective), and the level of automation of the attack. The authors also present other, less frequently discussed classification options, such as legal relevance, architectural level, or the stages of the attack (based on the kill chain model). Special attention is given to abuses observable through payment transactions, which primarily affect end-users. The research highlights that strengthening technological protection and law enforcement is not sufficient: there is also a need to improve financial awareness and cybersecurity knowledge.

JEL codes: E50, K24, K49

Keywords: cybercrime, grouping, banking

1 *Milán Kiss* PhD student, University of Miskolc, corresponding author. E-mail: milan.kiss@student.uni-miskolc.hu.
Levente Kovács Secretary General, Hungarian Banking Association; Head of Department, University of Miskolc. E-mail: kovacs.levente@bankszovetseg.hu.

1 INTRODUCTION

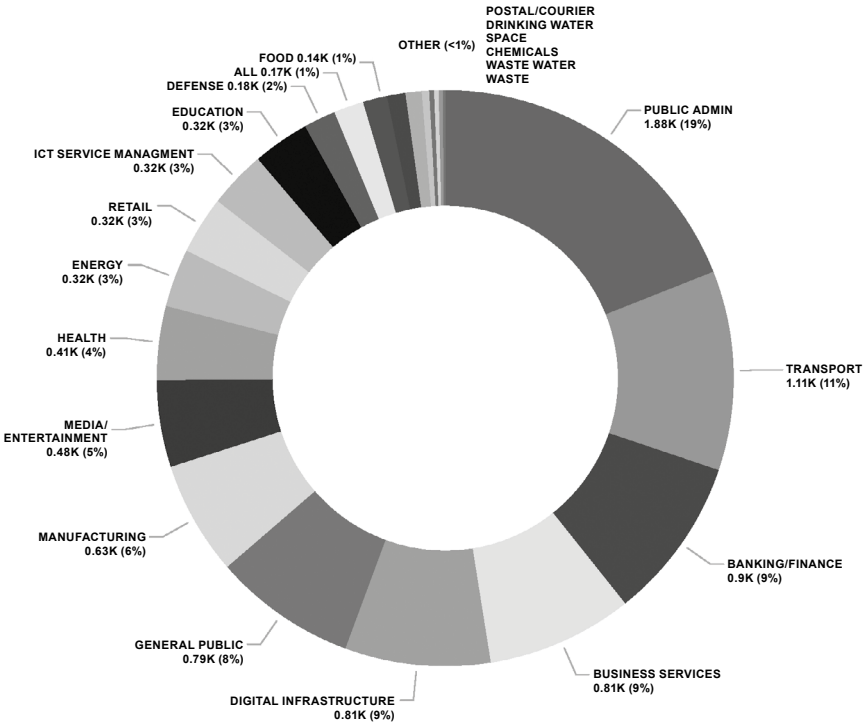
Cybercrime, including financial-type abuses, has a significant impact on the national economy and on overall confidence in the financial system. Therefore, it is particularly important to examine them so that law enforcement authorities, the various supervisory authorities, financial institutions and users of financial services can effectively combat or defend themselves against these abuses. It is also important to ensure that the education of the next generation of cybersecurity professionals will be of a high standard. In order to raise the effectiveness of defence and prevention to an adequate level, it may be necessary to develop a taxonomy that enables transparent classification, that is, the classification of abuses committed in cyberspace. Such a classification may assist legislators in drafting appropriate legal texts, as well as cybersecurity experts when designing cybersecurity systems. It may further contribute to making communication, and in particular customer education, more effective, whether at the level of individual payment service providers or in the case of collective action[2]. In addition, it may help instructors within universities and other vocational training programmes to support understanding and learning more effectively through the materials they prepare or present.

In recent years and decades, financial crime has changed. Crimes committed in physical space, such as money theft, bank robbery, have moved into cyberspace (Jaishankar, 2007). As Mastercard notes in its publication *The Age of Cybercrime*, "[c]ybercrime is like any other crime, and we must address it accordingly. If it brings money, it flourishes"; all this while these property crimes have become international (Mastercard, 2025). As a result, cybercrime has become one of the most pressing problems of our time. Hardly a day goes by that we don't hear or read a news story in some online or offline media about a crime or cyber-attack in the online space. According to the information available on the website of the Supervisory Authority for Regulatory Affairs, thirteen thousand people in Hungary were victims of cybercrime in 2024, causing financial losses of around HUF 30 billion (SZTFH, 2024), while the National Bank of Hungary (MNB) cites losses of nearly HUF 42 billion (MNB, 2025b). While there is a large latency in the data, it is clear that cybercrime has become a significant and widespread problem by the 2020s. However, cybercrime does not affect different economic sectors in the same way. According to the European Union Agency for Cybersecurity (ENISA), around 19 percent of cyber attacks target the public sector, while 11 percent and 9 percent target transport and financial services respectively. The main threats are ransomware, malware, social engineering, data breaches, distributed denial-of-

2 See e.g. the CyberShield initiative at https://kiberpajzs.hu/.

service (DDoS), information manipulation and compromise, and supply chain attacks (ENISA, 2024).

Figure 1
Sectors targeted by cyberattacks by number of incidents (July 2023 – June 2024)



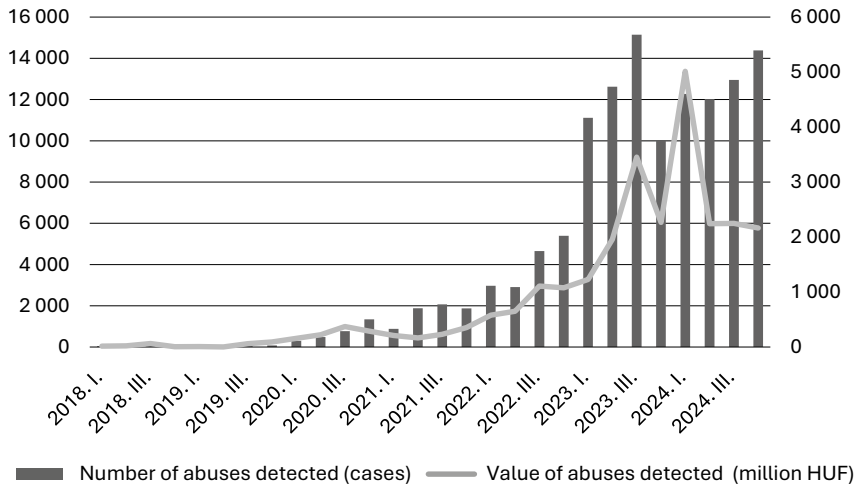
Source: (ENISA, 2024)

In the case of the financial sector, it can be observed that successful cyberattacks typically do not affect financial organisations, i.e. the service providers, but rather the clients making use of financial services. This may primarily be due to the fact that in Hungary the legal framework relating to IT security is highly developed[3],

3 The European legislator established, by adopting Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Digital Operational Resilience Act – DORA), a unified set of requirements similar to the earlier Hungarian regulation.

and the financial sector largely complies with these legal requirements (MNB, 2022). In other words, "general" cyberthreats manifest in a specific way in the financial sector. Thus, it can be stated that, for example, hacking a bank or an organisation operating a payment system may be very difficult, whereas a comparable level of protection is not always ensured on the client side. Consequently, perpetrators of cyberattacks primarily target the clients using financial services. These abuses can mainly be observed through (electronic) payment transactions, since the perpetrators are able to obtain the misappropriated funds through payment systems.

Figure 2
Number and value of abuses detected in financial transactions



Source: (MNB, 2025a)

Figure 2 shows that, unfortunately, the number and value of abuses in financial transactions has increased steadily in recent years. According to the data of the National Bank of Hungary, successfully executed fraud cases have been on the rise, and even after adjusting the figures for the last few quarters, their aggregate value remains remarkably high.

2 CLASSIFICATION CRITERIA FOR CYBER THREATS

There are many studies in the literature that classify cybercrimes according to some criteria. Examples of such studies include (Gordon–Ford, 2006; Onwubiko, 2020; Nagy, 2022), however, these studies are rather abstract, meaning that they tend to focus on cyberattacks, which include everything from attacks against information systems to pornographic content. All of this is of course useful for law enforcement and regulatory authorities, but less relevant for financial institutions from a practical point of view.

Accordingly, defining categories that enhance practical applicability for financial institutions and their supervisory authorities, developers of cybersecurity curricula and communications, and legislators responsible for drafting financial legislation is warranted.

2.1 Classification by attack method[4]

Cybercrimes can be grouped by the type of attack. This approach examines the nature of the attack or threat that the target group is facing. The categories are mainly distinguished by the means of attack.

Three categories of threats can be distinguished:

- Malware attacks:

  In the context of malware attacks, malicious code is installed on the victim's device (e.g., ransomware – software that attempts to extort money from the user by means of threats; adware – programs that display unsolicited advertisements, sometimes combined with surveillance; keyloggers – programs that record keystrokes to obtain sensitive information; killware – malicious software capable of causing physical harm, for example in attacks against hospitals). Related terms: adware, backdoor, beaconing, binder, bot, botnet, cryptojacking, cryptotrojan, dkom, exploit, worm, keylogger, killware, ransomware, time bomb, trojan, virus, worm.

- Social engineering:

  In this case, the user of the IT device is targeted and attempts are made to influence them (e.g., phishing – deceptive emails aimed at obtaining confidential

4 For each classification aspect, examples are given and explained to help the proper understanding of the aspect concerned. This is followed by a list of terms in that category. Explanations of the terms in the list can be found in the Cyber Security Glossary (2025) compiled by Kovács-Terták, published in this thematic issue.

information; baiting – luring the victim with promises of gifts or downloads; whaling – targeting high-profile individuals, such as CEOs, in a deceptive manner). These attacks often exploit human greed, appealing to promises of prizes or investments promising exceptionally high returns. Related terms: phishing, angler phishing, baiting, whaling, business email compromise, targeted phishing, doxing, evil twin phishing, hoax, phishing, smishing, spoofing, vishing, whaling.

- Other attacks:

  They mainly concern weaknesses or vulnerabilities in IT systems (DoS/DDoS – attacks that overload the IT system; zero-day attacks – exploits of unknown vulnerabilities; exploits – targeted code snippets to exploit vulnerabilities). Related terms: DoS/DDoS attack, exploit, zero-day attack, SQL injection, cross-site scripting, DNS spoofing, DNS tunneling.

The means of attack can therefore be malicious code written by someone, exploiting an existing IT vulnerability, or directly attacking the user.

2.2 Classification by attacker profile

Classification by attacker profile is a human-centred approach to organising cyber threats, which categorises attackers based on their intentions, capabilities, level of organisation, and resources. This perspective is particularly useful for risk assessment, developing defensive strategies, and threat modelling. Attackers possess varying motivations, expertise, and toolsets. Based on these characteristics, the following main categories can be distinguished:

- State-Sponsored / Advanced Threat Actors (APT – Advanced Persistent Threat):

  Organised groups, often with state or military backing, that demonstrate a high level of technical sophistication (e.g., developing their own exploitation methods and so-called zero-day attacks). They typically conduct long-term, covert, and targeted operations. Their targets generally include governmental bodies, the defence industry, large corporations, and critical infrastructure, such as financial infrastructures and payment service providers. Related terms: APT, cyber warfare, cyber weapon.

- Organised criminal groups:

  These are typically "for-profit" organisations, with the aim of obtaining data for monetary or financial extortion. They take advantage of phishing, BEC (Business Email Compromise), malware, zombie networks. In many cases, they operate as a "service" (e.g. malware-as-a-service), enabling even less

skilled cybercriminals to cause great damage. Related terms: business email compromise, bot, botnet, cryptojacking, cryptotrojan, black hat hacker.

- Hacktivists:

  Typically, they pursue political or ideological goals, which are achieved by hacking into IT systems, hacking into websites, leaking data or changing the appearance of websites (website defacement). Their aim is mostly to raise awareness, not necessarily to make a financial profit. Related terms: hacktivist, doxing.

- Script kiddies:

  They have little technical knowledge of their own, usually using code and software written by others. Their goals can be: fame, entertainment, revenge. An example of such an attack is the 15-year-old boy who "hacked" the Hungarian Educational Administration and Information System (KRÉTA). Related term: phishing.

In the context of the above classification, it is also worth mentioning ethical hackers and security professionals who, with the right permissions, test the security of certain systems in a legal framework with the aim of improving the protection of IT systems. An example of such a test could be a penetration test, or a test required by law or directly applicable legislative act of the European Union (e.g. threat-led penetration testing (TLPT) referred to in Article 26 of DORA).

2.3 Classification by type of target

Cyber threats can target different types of actors: individuals, businesses (micro, SMEs, but also large enterprises), or even infrastructures of critical national security importance.

- Cyberattacks against natural persons:

  In addition to financial abuse, these attacks typically aim to obtain personal data or steal private information. Typical attacks include keylogging, phishing, doxing (disclosure of personal or organisational information to discredit the person or organisation concerned), Nigerian-style scams (scamming money with a romantic or charity story), cyberbullying (online harassment via social networking platforms or other messaging applications). Attacks exploiting human greed (such as promises of unexpected prizes or investments promising high returns) are also common. Related terms: keylogger, phishing, doxing, cyberbullying, evil twin phishing, angler phishing, baiting, smishing, vishing, spoofing.

- Businesses:

  Attacks against businesses or other organisations, such as foundations or non-profit organisations[5], are primarily aimed at making money by stealing business data, crippling systems for ransomware, compromising supply chains, gaining competitive advantage or leaking confidential data. Typical attacks may include Business Email Compromise (BEC) – manipulation of corporate emails, fraud involving falsified invoice information, spear phishing/whaling – that is, targeted phishing against decision-makers, as well as attacks using malicious code (e.g., ransomware, which involves encrypting files and demanding a ransom for their release). Related terms: business email compromise, spear phishing, whaling, ransomware, cryptojacking, botnet, backdoor, exploit, binder, payload.

- Critical infrastructures:

  These sectors are essential for society to function: health, transport, energy, water, government systems, etc. In the case of financial institutions, examples include payment and securities settlement systems[6], but also credit institutions with a significant retail customer base. The attacks are usually aimed at causing physical or economic damage, political destabilisation or disruption of services to the population. Attacks are typically carried out via killware, APT attacks and DoS/DDoS attacks. Related terms: APT, DoS/DDoS, cyber weapon, cyber warfare.

Differentiation by target is very important, as attacked entities possess varying levels of protection and response capabilities. Protecting the general public naturally requires entirely different measures than, for example, ensuring the security of Hungary's payment systems.

5 Some research and development organisations that operate in high value-added sectors in the European Union function as non-profit entities or foundations.

6 The infrastructures of Real-Time Gross Settlement System (VIBER) operated by the Hungarian National Bank (MNB), the Interbank Clearing System (BKR) operated by GIRO Elszámolásforgalmi Zrt., and KELER Central Securities Depository Ltd. and KELER KSZF Központi Szerződő Fél Zrt. related to securities settlement and record-keeping.

2.4 Classification by phase of defence

IT system protection can be divided into three distinct parts (Gyaraki, 2023).

- Preventive actions:

  These measures are designed to prevent attacks, i.e. to prevent attackers from gaining access to the IT system. Preventive controls can be physical intrusion prevention, administrative or some logical controls. Related terms: Anti-phishing, Bug bounty.

- Detective actions:

  Their aim is to make attacks "known", i.e. they cannot intervene, but they make the cyber attack visible. Related terms: IDS, SIEM.

- Corrective actions:

  Measures taken in response to a detected cyberattack to stop the extension of the attack or the attack itself and prevent further damage. Related terms: CIRT.

2.5 Classification by the type of tool used for the attack

One fundamental characteristic of attacks is the extent to which they rely on automation versus requiring human involvement and decision-making. The two main categories are automated and manual/interactive attacks. It should be noted that categorising certain tools, such as those using artificial intelligence, can be challenging.

- Automated attacks:

  These attacks typically occur on a large scale, executing thousands or even millions of attempts against a target. They generally require little to no human intervention, and are fast, repeatable, and scalable. An example of such an attack is a botnet attack, which involves a network of infected devices controlled by a central operator. Botnets are used to carry out DDoS attacks, send spam, or perform so-called brute force password attacks, where access to IT systems is attempted through simple trial-and-error methods. Related terms: botnet, DDoS attack, cryptojacking, ransomware, brute force, worm, beaconing, backdoor, spam, exploit.

- Manual attacks:

  Manual attacks are usually targeted, often against specific organisations or individuals. Manual attacks require human observation, decision-making and tactical planning. They are characterised by detailed preparation and in-

telligent execution. They are often part of a complex chain of attacks. Types may include, for example, spear phishing, which is a phishing attack tailored specifically to an organisation or an individual. After gathering information, targeted emails are sent, often to executives (phishing targeting executives is called whaling). The attacker patiently builds trust and then tries to obtain sensitive data. Related terms: spear phishing, whaling, phishing, doxing, angler phishing, evil twin phishing, baiting, smishing, vishing, social engineering.

The two types of attack may require different types of defence.

2.6 Other classification criteria

In addition to the main classification criteria described above, further dimensions can be used to classify cybersecurity terms. They help to gain a deeper understanding of the threats and fine-tune defence strategies.

a) The place of the attack in the IT architecture

Another consideration is which IT component is targeted by the attack:

- Client-side attacks: In this case, the target is the device or software used by the user. This type of threat could be adware (ad-based software) or a keylogger that records the user's keystrokes. Related terms: adware, keylogger, baiting, phishing, doxing, smishing, vishing, angler phishing, evil twin phishing, spyware, ransomware (if it encrypts client-side files).
- Server-side attacks: In this case, the system providing the service (e.g. web or database server) is attacked. Typical examples: DoS attacks (denial of service attacks), ransomware. Related terms: DoS/DoS attacks, ransomware, backdoor, exploit, brute force.
- Network level attacks: in this case, the target of the attack is communication and data transfer. Typical examples are DNS tunnelling, where the DNS protocol is used to transfer malware, or the evil twin phenomenon, where a fake Wi-Fi network is created to deceive victims. Related terms: DNS tunnelling, evil twin phishing, spoofing, beaconing, mitm (man-in-the-middle), sniffing.

This classification may be of particular relevance to IT security experts, as the devices to be protected form the basis of the classification. It should be noted, however, that for the so-called zero trust security strategy the classification is not relevant.

b) Legislative approach

Another consideration may be whether the given act is legally permitted, prohibited, or subject to uncertain judgement:

- Specifically punishable offences: This category includes, for example, the cloning of payment cards, which under criminal law constitutes an abuse of a non-cash payment instrument. It should be noted that in some cases the criminal-law classification of a given act is not unequivocal; phishing is an example (Biró–Kiss, 2024). Related terms: phishing, spear phishing, whaling, ransomware, keylogger, backdoor, botnet, DDoS attack, DoS attack, spoofing, smishing, vishing, angler phishing, evil-twin phishing, cryptojacking, exploit, doxing.
- Lawful activity within specialised frameworks: Ethical hacking carried out under contract or other agreement (e.g., penetration testing) may also be performed to meet statutory requirements and is therefore not punishable but mandated. Related terms: ethical hacking, bug bounty.
- Grey zone: The application of OSINT (Open Source Intelligence), i.e. the collection of publicly available information for intelligence purposes, may in some cases fall into a risky area, since it is not legally prohibited but may be morally unjustifiable. Related terms: OSINT, cyber threat intelligence, gray hat hacker, digital footprint collection.

This type of classification may be of relevance to legislators and financial institutions and authorities that apply the law, as it can be a basis for identifying loopholes and protecting financial sector secrets.

c) By the nature of the term

Cybersecurity terms can also be categorised by their nature.

- Technical terms: E.g. exploit, malware, which are technical IT terms. Related terms: exploit, malware, ransomware, keylogger, botnet, backdoor, DNS spoofing, dns tunneling, ddos attack, dos attack, beaconing, brute force, payload, phishing, spear phishing, spam, VPN, SSL, TLS, IDS, IPS, antivirus, Indicator of Compromise, cyber weapon, firewall, sniffin.
- Colloquial or slang terms: E.g. hoax, which means fake news or misleading content, mainly used to manipulate users. Related terms: hoax, baiting, smishing, vishing, evil twin phishing, angler phishing, gray hat hacker, black hat hacker, white hat hacker, script kiddie, whaling, hacker, spoofing.
- Legal terminology: e.g. electronic information system, electronic money, non-cash payment instrument, defined by legislation or European Union legislative acts. Related terms: cybercrime, ethical hacking, digital footprint, personal data, information system, OSINT.

These additional aspects allow for a multidimensional examination of terms, which can help to provide a more complex analysis of cybersecurity threats and to develop more effective regulatory, educational and defence mechanisms.

d) By the phase of the attack

Classification by the phases of the attack is one of the most frequently applied methods for understanding and modelling complex, targeted cyberattacks. This approach was established by the well-known Cyber Kill Chain model (Lockheed Martin, 2025), which clearly illustrates how an attack unfolds step by step.

According to the model, an attack comprises the following phases:

- Reconnaissance: the attacker collects information about the target, its systems, personnel, email addresses and technological environment. The objective is to understand the target's operation so that the attack can be tailored. Related terms: OSINT, doxing, social engineering, whaling, spear phishing.
- Entry / Initialisation: the attacker selects and deploys the vector that enables access, for example by means of social engineering. Its objective is to introduce malicious code or to persuade the user to "open the door". Related terms: phishing, smishing, vishing, baiting, angler phishing, evil twin phishing, spoofing, malware, exploit.
- Installation: The attacker establishes stable access and tries to gain higher privileges/access rights. From there it "starts moving" within the network. The aim: to ensure access to deeper layers of infrastructure and to hide the presence. Related terms: backdoor, keylogger, botnet, cryptojacking, ransomware, beaconing, worm, binder, rootkit, payload.
- Achieve the objective and exit: The attacker executes its real purpose (e.g. data theft, extortion) and then leaves the system – preferably without a trace. The aim of this phase is to obtain data, to extort or to achieve other attack objectives, while minimising the risk of detection. Related terms: data exfiltration, ransomware, spyware, identity theft, exfiltration, killware.

Of course, beyond the classification criteria listed above, numerous other classification schemes are conceivable (e.g., the MITRE ATT&CK® framework[7]).

7 See the website at https://attack.mitre.org/.

3 ABUSES OBSERVED THROUGH PAYMENT TRANSACTIONS

The National Bank of Hungary has repeatedly declared that the Hungarian financial system is considered safe even by European standards (MNB, 2023). This is one of the reasons why the title of Recommendation 5/2023 (VI.23.) of the National Bank of Hungary (the Anti-fraud Recommendation) refers to abuses observable through payment services, rather than abuses affecting payment services. Nevertheless, customers using payment services may encounter cybercrime. These cybercrimes can be categorised in accordance with the classifications outlined above.

Table 1
The most common types of abuse observed through payment transactions

Business Email Compromise	Businesses	E-mail, invoice	Transfer manipulation
CEO-fraud / Social engineering	Finance of enterprises	E-mail, psychological manipulation	Initiating a transfer from within
Phishing / Smishing / Vishing	Individuals	E-mail, SMS, telephone	Access by stealing data
Card fraud	Payment service providers' customers	Card details	Unauthorised purchase
Fake online shops	Customers	Fake page	Obtaining money or data
Ransomware	Businesses, institutions	Malicious code and cryptocurrency payments	Ransom
Prepayment fraud	Anyone	E-Mail	Swindling money for a promise

Source: (OECD 2022; CISA 2023; FBI 2023; Kovács–Terták, 2024)

It should also be noted that the attack methods presented in *Table 1* are only the most common as of summer 2025. Of course, as with cyberattacks in general, the phenomenon of payment fraud is constantly evolving. Whereas in 2020 traditional methods predominated, such as the physical theft of customers' payment cards, by 2025 significantly more sophisticated frauds have become more common, and the use of artificial intelligence is no longer uncommon. For example, within the framework of the so-called Matrix project, the police dismantled a group operating a system similar to bank customer centres (ORFK, 2024).

On the basis of the above, it can be stated that the most common cyber frauds, which also affect financial institutions, can be classified according to several of the classifications presented earlier. It can further be established that such classifications are necessary, as they may significantly facilitate protection against fraud by enabling more effective communication and clearer legislation.

Defending against fraud is by no means simple. Everyday financial experience highlights the importance of improving financial awareness, as emphasised in the study by Hergár, Kovács and Németh (2024). Other authors, by contrast, underscore the opportunities offered by technology and legislation (Doeland, 2019). Since the transposition of the Payment Services Directive 2[8] (PSD2) into Hungarian law and the introduction of instant transfers, the national regulator, the National Bank of Hungary, has sought to combat fraud prevention through a complex four-pillar framework (Kiss, 2023).

SUMMARY

The study provides an overview of the current state of cybercrime affecting the financial sector, the possibilities for its classification, and the necessity of defence mechanisms. The increasing prominence of the digital sphere, the electronic management of everyday finances, and the expansion of online services have significantly heightened the likelihood of cyberattacks, and, in parallel, their gravity and socio-economic impact.

The opening chapters highlight that over the past decade the structure of crime has shifted markedly from the physical domain into cyberspace. This change is particularly evident in the field of financial fraud, where traditional offences – such as robbery – have been replaced by online abuses and attacks supported by technological tools. The study emphasises that the IT protection of Hungarian financial institutions is advanced even by European standards; as a result, a significant proportion of attacks target customers, who have fewer resources available for protection, lower self-defence capabilities, and are often inadequately informed.

The research applies a systematic approach aimed at offering comprehensive and practically applicable classifications of types of cybercrime. This approach is implemented along several dimensions:

By attack method: distinguishing between technical attacks (malware, exploit), user-deception-based attacks (phishing, baiting), and those exploiting system

8 Directive (EU) 2015/2366 of the European Parliament and of the Council.

vulnerabilities (DoS/DDoS, zero-day). This classification facilitates the targeted development of defence mechanisms, as a technical attack requires a different approach from one based on psychological manipulation.

1. By attacker profile: classification is made based on the motivation, tools, and organisational level of attackers. State-sponsored APTs, organised criminal groups, hacktivists, and less skilled script kiddies pose varying levels of risk and threat. Typifying attackers is particularly important for targeted prevention and threat modelling.
2. By target type: natural persons, businesses, and critical infrastructures are subject to attacks of different nature and scale. The study presents in detail the types of fraud typical of these actors, ranging from keyloggers and phishing to ransomware attacks and supply chain compromises.
3. By phases of defence: system protection is divided into three components according to the classical classification – preventive, detective, and reactive controls.
4. By degree of the automation of the tools used for the attack: large-scale automated attacks, and targeted manual actions against individual entities.
5. Other classification criteria are also presented, such as legal relevance, the attacked device, or the phases of attack according to the so-called kill chain model.
6. The study pays particular attention to how fraud observable in payment transactions fits into the above classification framework. Practical examples – such as Business Email Compromise, phishing, CEO fraud, or fake online shops – clearly illustrate how attack forms intertwine technological and psychological manipulation, and at which points of the financial ecosystem they exert an impact.

The European Union's legislative acts, regulations, and non-binding recommendations introduced in recent years – particularly the PSD2, DORA, and the Anti-fraud Recommendation – reinforce the defence framework, yet the pace of technological development necessitates continuous adaptation. Defence cannot rely solely on technology; the enhancement of customers' financial awareness, education, and targeted communication campaigns are equally important.

For the successful fight against cybercrime, the development of a well-structured and practically applicable taxonomy is indispensable. This not only assists cybersecurity professionals and legislators, but also enables financial service providers and customers to gain a clearer understanding of the nature of threats and possible defence strategies.

One of the main merits of the study is that, unlike the more general approaches of the international literature, it focuses specifically on the particularities and practical needs of the financial sector. As a result, it applies classification criteria that can directly support the internal risk management, customer communication, and technological development processes of financial service providers.

Concluding thoughts

In the dynamically evolving environment of cyber threats, the effective support of law enforcement and prevention requires the coordinated, proactive and deliberate action of all actors in the financial sector – whether regulators, service providers or customers. One of the cornerstones of this path is the classification, understanding and prediction of attacks. The systematic approach presented provides a foundation on which effective future defence and regulatory structures can be built, serving financial stability, client security and the sustainability of the digital ecosystem alike.

REFERENCES

Biró, G. – Kiss, M. (2024): Adathalászat és az ellene történő egyes védekezési lehetőségek. *Gazdaság és Pénzügy* 11(4): 417–439. https://doi.org/10.33926/GP.2024.4.2.

CISA (2023): #StopRansomware Guide. https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf.

Doeland, M. (2019): How to keep payments safe and secure in a changing world. *Journal of Payments Strategy & Systems* 13(2): 132. https://doi.org/10.69554/FSLK7337.

ENISA (2024): ENISA threat landscape 2024: July 2023 to June 2024. *LU: Publications Office*. https://data.europa.eu/doi/10.2824/0710888.

FBI (2023): Internet Crime Report. https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf.

Gordon, S. – Ford, R. (2006): On the definition and classification of cybercrime. *Journal in Computer Virology* 2(1): 13–20. https://doi.org/10.1007/s11416-006-0015-z.

Gyaraki, R. (2023): Az információbiztonság alapjai. https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/az_informaciobiztonsag_alapjai_konyv_kesz_2.pdf.

Hergár, E. – Kovács, L. – Németh, E. (2024): A pénzügyi kultúra helyzete és fejlődése Magyarországon. *Hitelintézeti szemle* 23(1): 5–28. https://doi.org/10.25201/HSZ.23.1.5.

Jaishankar, K. (2007): Establishing a theory of cyber crimes. *International journal of cyber criminology* 1(2): 7–9. https://www.cybercrimejournal.com/IJCC-July-December-2007-Vol1-No2.php.

Kiss, M. (2023): Az MNB szerepe a pénzforgalmon keresztül megfigyelhető visszaélések kezelésében. *HANTOS PERIODIKA* 4(2): 279–290.

Kovács, L. – Terták, E. (2024): A kiberbűnözés legjobb ellenszere a pénzügyi műveltség. *Gazdaság és Pénzügy* 11(1): 6–29. https://doi.org/10.33926/GP.2024.1.2.

Lockheed Martin (2025): Cyber Kill Chain. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Mastercard (2025): A kiberbűnözés kora 2025. https://www.mastercard.hu/content/dam/public/mastercardcom/eu/hu/pdfs/A%2520kiberb%25C5%25B1n%25C3%25B6z%25C3%25A9s%2520ko

ra%25202025.pdf&ved=2ahUKEwjvkaPF09ONAxUt9rsIHeGvCQ0QFnoECBgQAQ&usg=AOvVaw1960KT7grbPA6T5Bb30sXw.

MNB (2022.12.): A magyar pénzügyi szektor kiberfenyegettségi térképe 2022. *Magyar Nemzeti Bank*. https://www.mnb.hu/letoltes/kiberfenyegetettsegi-terkep-2022.pdf.

MNB (June 2023): Fizetési Rendszer Jelentés 2023. *Magyar Nemzeti Bank*. https://www.mnb.hu/letoltes/fizetesi-rendszer-jelentes-2023-hun-0626.pdf.

MNB (2025a): Pénzforgalmi táblakészlet. https://statisztika.mnb.hu/publikacios-temak/penzforgalmi-adatok/penzforgalmi-adatkozlesek/tajekoztato---penzforgalom.

MNB (17 July 2025b): Fizetési Rendszer Jelentés 2025. *Magyar Nemzeti Bank*. https://www.mnb.hu/letoltes/mnb-fizetesi-rendszer-jelentes-2025-hun-digitalis-vegleges.pdf.

Nagy, Z. A. (2022): Kibernyomozói kézikönyv. Budapest: Nemzeti Közszolgálati Egyetem *Ludovika Egyetemi Kiadó*.

OECD (2022): Online Consumer Fraud in the Digital Age. https://one.oecd.org/document/DSTI/CP(2021)7/FINAL/en/pdf.

Onwubiko, C. (2020): Fraud matrix: A morphological and analysis-based classification and taxonomy of fraud. *Computers & Security* 96 101900. https://doi.org/10.1016/j.cose.2020.101900.

ORFK (2024): MÁTRIX Projekt: Borult az első Call Center. https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/matrix-projekt-borult-az-elso-call-center.

SZTFH (2024): Mintegy 30 milliárd forintnyi kárt okoztak a kibercsalások hazánkban. https://sztfh.hu/mintegy-30-milliard-forintnyi-kart-okoztak-a-kibercsalasok-hazankban/.